ELECOM apps

IKARUS mobile.security

取扱説明書

目次

はじめに……3
■パッケージ内容の確認……3
■動作環境について……3
■画面について……3
アプリのインストール……4
■インストールの流れ……4
端末の設定……5
ダウンロードとインストール……5
初期設定をする……7
シリアル番号の入力……7
チュートリアルの実行……9
USSD プロテクト機能の設定……10
リモートコントロールの設定……11
SMS フィルタリングの設定……14
Web フィルタリングの設定……16
初回スキャン……17
メイン画面について……18
情報エリア……18
アンチウィルス……19
監視……19
Web フィルタリング……19
盗難防止……20
テキストメッセージフィルタ……21
情報……21
チュートリアルウィザード……21
アンインストール……21
ウイルスや不正なアプリが見つかったら……22
リモートコントロールで端末を保護する……23
ライセンスの更新について……24
■更新ライセンスの入手方法……24
■更新ライセンスの登録方法……24
本製品のアップデート……26
本製品のアンインストール……27
こんなときは……28
商品に関するお問い合わせは……28

はじめに

このたびは、ELECOMApps「IKARUS mobile.security」をお買い上げいただきありがとうございます。
本マニュアルは、「IKARUS mobile.security」のダウンロード、インストール、設定方法について説明します。ご使用前に、必ずお読みください。

■パッケージ内容の確認

本製品のパッケージには次のものが入っています。作業を始める前に、すべてが揃っているかを確認してください。なお、梱包には万全を期しておりますが、万一不足品などがありましたら、すぐにお買い上げの販売店またはエレコム総合インフォメーションセンターまでご連絡ください。

●製品シリアル番号カード　1 枚　　●取扱説明書（本書）　1 部

本製品と同じ有償アプリを Play ストアで購入すると課金されますので、購入しないようご注意ください。

■動作環境について

本製品は下記の環境で動作します。

Android OS 2.3/4.0/4.1

■画面について

本マニュアルでの画面の説明は、スマートフォン端末での表示で説明しています。
タブレット端末の場合は、表示が異なりますが、操作手順や操作内容は同じです。

スマートフォン端末の場合

タブレット端末の場合

アプリのインストール

■インストールの流れ

各種ダウンロードのために、インターネット接続を行います。設定内容およびご契約内容によっては、パケット代が発生することがありますので、ご注意ください。

1 端末の設定
Android 端末に本製品をインストールできるように設定します。

2 IKARUS mobile.security のインストール
IKARUS mobile.security をダウンロード / インストールします。

3 シリアル番号の入力 / ライセンスの有効化
シリアル番号を入力して、本製品を使用できるようにします。

4 初期設定
チュートリアルウィザードにしたがって本製品を正しく使えるように設定していきます。

本マニュアルで使用されている画面は、Android 4.1 端末の例です。お使いの端末により、表示される内容が異なる場合があります。

1 端末の設定

Android 端末にアプリをインストールできるように設定します。

1 「設定」画面で［セキュリティ］をタッチします。

メモ Android 2.3 の端末をご使用の場合は、「設定」画面で［アプリケーション］をタッチしてください。

2 ［提供元不明のアプリ］をタッチして、チェックします。

メモ 設定方法について、詳しくはお使いのAndroid 端末のメーカーの取扱説明書をお読みになるか、メーカーにお問い合わせください。

Tips ［提供元不明のアプリ］の設定は、通常お買い上げ時の設定では「オフ」になっています。この状態では、「Play ストア」以外で提供されるアプリがインストールできなくなっています。

2 ダウンロードとインストール

アプリを弊社専用ページからダウンロードしてインストールします。

3 「IKARUS mobile.security」のダウンロードページにアクセスします。

ダウンロードページへのアクセスには、２つの方法があります。

❶以下の QR コードを撮影してアクセス

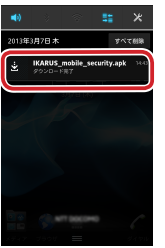
❷ URL をブラウザに直接入力

http://app.elecom.co.jp/dl/IKARUS_mobile_security.apk

4 「IKARUS mobile.security」のダウンロードを開始します。

5 **ステータスバーに↓マークが表示されたら、ステータスバーを下方向になぞって、通知パネルを開きます。**

6 **右の画面が表示されます。**
［IKARUS_mobile_security.apk］をタッチします。



7 **右の画面が表示されます。［インストール］をタッチします。**

8 **「IKARUS mobile.security」のインストールが終了します。**
このあと続いて、IKARUS mobile.security の設定をおこないます。
［開く］をタッチして、次の「IKARUS mobile.security の初期設定」に進んでください。

Tips

［完了］をタッチすると、インストール画面を閉じます。

初期設定をする

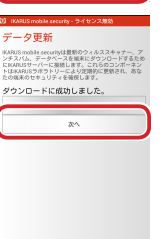
IKARUS mobile.security を使用するには、最初に IKARUS mobile.security を使用するため機能の設定が設定が必要になります。
IKARUS mobile.security では「チュートリアルウィザード」を用意しています。
「チュートリアルウィザード」では、画面の指示に従って進むだけで、機能の内容を把握しながら必要な設定ができます。

1 シリアル番号の入力

メモ シリアル番号は登録した端末１台でのみ利用可能です。

1 トップ画面で[承諾]をタッチします。

2 データ更新を開始します。終了したら[次へ]をタッチします。



3 シリアル番号を入力します。

同梱の「シリアル番号カード」に記載されている製品のシリアル番号（16 桁）入力します。

❶[QR コードをスキャン]をタッチします。

❷表示される画面で「シリアル番号カード」に記載されているシリアル番号の QR コードを撮影します。
「シリアル番号欄」にシリアル番号が入力されます。

❸[ライセンスを有効にする]をタッチしてシリアル番号を登録します。

Tips

「シリアル番号欄」にシリアル番号を直接入力することもできます。

認証済の端末では本製品のシリアル番号は利用できません。
更新用のシリアル番号をご利用ください。

有効なライセンスが確認されると、チュートリアルウィザード画面に進みます。「2 チュートリアルの実行」に進んでください。

2 チュートリアルの実行

4 チュートリアルを実行するかどうかを確認する画面が表示されます。

このチュートリアルを利用すると、下記の順序で、本製品の基本機能を確認しながら、必要な設定が行えます。

- USSD プロテクト
- 遠隔操作 / 盗難防止
- 遠隔操作のパスワード
- SMS フィルタリング
- Web フィルタリング

5 [次へ]をタッチします。

USSD プロテクト機能の設定画面に移ります。

メモ [スキップ]をタッチすると、チュートリアルを実行せず、初回スキャン実行画面が表示されます。(17 ページ)
基本メニュー画面の「チュートリアルウィザード」で本ウィザードを再実行できます。(21 ページ)
必要な設定は、基本メニュー画面からも行なうこともできます。(18 ページ)

3 USSD プロテクト機能の設定

USSD プロテクト機能とは、ウェブサイトの tel: リンクにタッチすると端末のデータが全消去されてしまうなどの脅威から Android 端末を保護する機能です。アクセス中のサイトに有害な USSD コードが含まれていないかを常に監視します。
※電話機能を持った端末でのみ利用できます。

6 **USSD プロテクト機能の概要を確認し、[有効]を選択してから[次へ]をタッチします。**

メモ [無効]を選択して、[次へ]をタッチすると、リモートコントロールの設定画面(11ページ)に移ります。

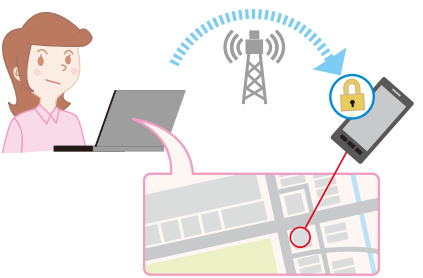
7 **[OK]をタッチします。**

8 **アプリケーションの選択画面で、「常にこの操作で使用する」をチェックして、[IKARUS mobile.security]をタッチします。**
リモートコントロールの設定に移ります。

4 リモートコントロールの設定

リモートコントロール機能を利用すると、Android 端末を紛失した場合などに、他の端末から SMS(ショートメッセージ)でコマンドを送信して盗難や不正使用を防止することができます。

・端末のデータ消去
・端末のブロック
・場所の特定
・アラーム
・SIM ロック



9 **リモートコントロール機能の概要を確認し、[有効]を選択してから[次へ]をタッチします。**

メモ [無効]を選択して、[次へ]をタッチすると、SMS フィルタリングの設定画面(14ページ)に移ります。

10 **右の画面が表示されます。[OK]をタッチします。**

11 デバイス管理者を有効にする画面が表示されたら[有効にする]をタッチします。

12 アプリケーションの選択画面で、「常にこの操作で使用する」をチェックして、[IKARUS mobile.security]をタッチします。

13 遠隔操作を設定するためのパスワードを入力し、確認のための再入力をして、[Next]をタッチします。

メモ パスワードは、6 文字以上 15 文字以内で入力してください。アルファベットと数字が使用できます。
アルファベットと数字は必ず 1 文字以上必要です。

Tips 「パスワードをテキストで表示」をチェックするとパスワードがテキストで表示されます。

14 リモートコントロールの項目を確認します。

設定できるリモートコントロールは次の 4 種類です。

データ消去：wipe:[password] と電話番号にテキストを送信することで、個人データはただちに削除されます。

端末のロック：lock:[password] と電話番号にテキストを送信することで、端末はただちにロックされます。

端末の探索：locate:[password] と電話番号にテキストを送信することで、端末の現在位置情報を Google マップリンクから取得できます。

アラーム：alarm:[password] と電話番号にテキストを送信することで、端末はアラームを発信します。また、パスワード入力以外でアラームを停止することはできません。

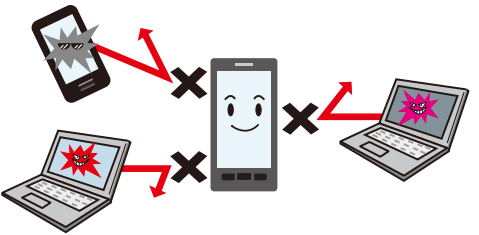
メモ リモートコントロールの操作の方法については、「リモートコントロールで端末を保護する」（23 ページ）をご覧ください。

15 [次へ]をタッチします。

SMS フィルタリングの設定画面に移ります。

5 SMS フィルタリングの設定

SMS フィルタリングとは、迷惑 SMS(ショートメッセージ)の拒否ができる機能です。
ブラックリストに特定の相手を登録することで、着信を拒否することができます。
また、返信内容を入力し、登録しておく機能もあります。



16 **SMS フィルタリングの概要を確認し、[有効]を選択してから[次へ]をタッチします。**

メモ [無効]を選択して、[次へ]をタッチすると、Web フィルタリングの設定画面(16ページ)に移ります。

テキストメッセージのブラックリストの登録画面が表示されます。

17 **「メッセージ履歴」タブをタッチします。**

着信履歴からブラックリストの登録をする画面が表示されます。

18 ブラックリストに登録する着信履歴をチェックします。

メモ 着信履歴からの選択は一部端末では利用できない場合があります。

Tips [連絡先を選択]タブにタッチして、電話番号や連絡先に登録してある名前を直接入力し[追加]をタッチして、登録することもできます。

19 [次へ]をタッチします。

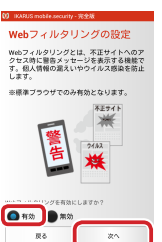
Web フィルタリングの設定画面に移ります。

6 Web フィルタリングの設定

Web フィルタリングとは、不正サイトへのアクセス時に警告メッセージを表示する機能です。個人情報の漏えいやウイルス感染を防止します。
※標準ブラウザでのみ有効となります。

20 Web フィルタリングの概要を確認し、[有効]を選択してから[次へ]をタッチします。

メモ [無効]を選択して、[次へ]をタッチすると、初回スキャン画面(17 ページ)に移ります。



7 初回スキャン

21 **設定終了のメッセージを確認し、端末全体のスキャンを行う場合は、[はい]をタッチします。**

22 **メイン画面が表示され、スキャンが開始されます。**

これで、IKARUS mobile.security の設定は終わりました。

メイン画面から設定できる機能について詳しくは、「メイン画面について」（18 ページ）をご覧ください。

メイン画面について

IKARUS mobile.security 起動すると、次のようにメイン画面が表示されます。
ここでは。メイン画面の機能について説明します。

情報エリア

IKARUS mobile.security の状態を表示します。

システムは保護されています

正しく動作しています。

システムは感染しています

ウィルスや不正なアプリが発見されました。

XXXXXX は無効になっています

XXXXXX(機能によって異なります)が、無効になっていて本製品の一部の機能が正しく使用できない状態になっています。

アンチウィルス

アンチウィルスについての操作、設定をおこないます。

- アプリのスキャンを開始します。
- 端末のフルスキャンを開始します。
- 自動スキャンを有効にします。
- 自動スキャンのモードを設定します。
  フルスキャン : 端末全体をデータを含めてスキャン
  アプリスキャン : インストールされているアプリをスキャン
- スキャンの頻度を選択します。
- ウイルスに感染の状況を確認します。
- アクティブなときは「ウイルスや不正なアプリが見つかったら」(22 ページ)をお読みください。
- ウイルス定義の更新を手動で行います。
- 無線 LAN 接続時のみウイルス定義の更新を行います。
- ウイルス定義の自動更新を有効にします。
- ウイルス定義の自動更新の頻度を選択します。
- 開発者に匿名でウィルスの情報を送信します。

監視

- 新規にインストールされたアプリや更新されたアプリの監視を有効にします。
- メモリーカード内のデータの監視を有効にします。
- USSD プロテクトを有効にします。

USSD プロテクトについて詳しくは、「3 USSD プロテクト機能の設定」(10 ページ)をご覧ください。

Web フィルタリング

Web フィルタリングについて詳しくは、「6 Web フィルタリングの設定」(16 ページ)をご覧ください。

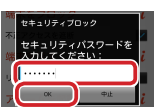
- Web フィルタリングを有効にします。

盗難防止

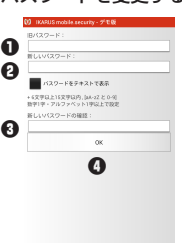
リモートコントロールについて詳しくは、「4 リモートコントロールの設定」(11 ページ)をご覧ください。

- 端末のデータをすべて消去します。
- 端末を操作できないようにします。
- GPS がオンになっている場合に、端末の場所を表示します。
- 離れた場所にある端末からアラーム音を鳴らします。
- SIM カードを抜いたときに端末を操作できないようにします。
- セキュリティパスワードを変更します。

メモ チェックを ON/OFF するたびにパスワードの入力を求められます。
パスワードを入力して、[OK]にタッチしてください。



パスワードを変更するには



❶現在のパスワードを入力します。

❷新しいパスワードを入力します。

メモ パスワードは、6 文字以上 15 文字以内で入力してください。アルファベットと数字が使用できます。
アルファベットと数字は必ず 1 文字以上必要です。

Tips 「パスワードをテキストで表示」をチェックするとパスワードがテキストで表示されます。

❸新しいパスワードをもう一度入力します。

❹[OK]にタッチします。

テキストメッセージフィルタ

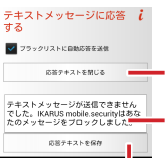
SMS フィルタリングについて詳しくは、「5 SMS フィルタリングの設定」（14 ページ）をご覧ください。

SMS フィルタリングを有効にします。

タッチしてフィルターする電話番号のリストを編集します。
詳しくは「5 SMS フィルタリングの設定」（14 ページ）をご覧ください。

SMS の受信を拒否する相手にテキストメッセージを送信します。

タッチして送信するテキストメッセージを編集します。



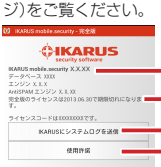
タッチして編集ウィンドを閉じます。

テキストメッセージを入力 / 編集します。

タッチしてテキストメッセージを保存します。

情報

IKARUS mobile.security のライセンスの期限を表示します。
ライセンスの更新については、「ライセンスの更新について」（24 ページ）をご覧ください。



本製品のバージョンを表示します。

ライセンスの期限を表示します。

IKARUS にシステムログを送信します。

タッチするとライセンス同意条項が表示されます。

チュートリアルウィザード

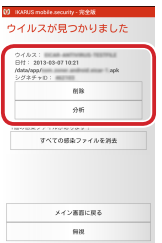
チュートリアルウィザードを使用し、再設定を行います。

アンインストール

IKARUS mobile.security をアンインストールします。
アンインストールについては、「本製品のアンインストール」（27 ページ）をご覧ください。

ウイルスや不正なアプリが見つかったら

お使いの端末にウィルスや不正なアプリが、見つかったら次の画面が表示されます。



検出されたウィルスや不正なアプリは、次の手順で処理してください。

1 **検出されたウィルスや不正アプリを削除する場合は[削除]をタッチします。[すべての感染ファイルを消去]をタッチすると、検出されたすべてのウィルスや不正アプリを削除できます。**

2 **アプリのアンインストール画面が表示された場合は、画面の指示にしたがってアプリをアンインストールします。**

リモートコントロールで端末を保護する

Android 端末を紛失した場合に、次の手順で他の端末から SMS(ショートメッセージ)でコマンドを送信して盗難や不正使用を防止します。

1 他の端末で、SMS を送信するアプリを起動します。

2 宛先にご使用の端末の電話番号を入力します。

3 メッセージ本文に下記のフォーマットで入力します。

（コマンド）：（パスワード）

設定したパスワードを入力します。

遠隔操作の動作に合わせたコマンドを入力します。

データ消去	wipe
端末のロック	lock
端末の探索	locate
アラーム	alarm

4 SMS を送信します。

リモートコマンドを送信して盗難保護機能を動作させるには、あらかじめ「盗難防止」の機能を有効にしておく必要があります。また、「端末の検索」を使用するには、端末の GPS 機能が ON になっている必要があります。
メイン画面の「盗難防止」(20 ページ)をお読みください。

例 「データ消去」コマンドで、パスワードが「password」の場合

wipe : password

ライセンスの更新について

お買い上げの際のライセンスは、1 年間です。続けて本製品を使用する場合は、更新ライセンスを購入していただくことになります。

■更新ライセンスの入手方法

更新ライセンスは、下記の弊社購入サイトで購入できます。

http://appstore.elecom.co.jp/ikarus/update_license.html

■更新ライセンスの登録方法

1 **ステータスバーに▲マークが表示されたら、ステータスバーを下方向になぞって、通知パネルを開きます。**

2 **「ライセンスの有効期限が近づきました」というメッセージが表示されます。**
表示されたメッセージをタッチします。

3 **[シリアル番号の入力 / 読み取り]をタッチします。**
シリアル番号を入力する画面が表示されます。

4 **シリアル番号を入力します。**

シリアル番号欄に新しく購入したライセンスのシリアル番号を入力するか、[QR コードをスキャン]をタッチして、弊社購入サイトで表示される QR コードを読み取ります。

5 **[ライセンスを有効にする]をタッチします。**

6 **シリアル番号の登録が正しく終了すると、「情報」画面が表示されます。**

ライセンス期限が更新されていることを確認してください。

本製品のアップデート

本製品のプログラムに更新がある場合は、次の手順で最新プログラムを入手します。

1 **ステータスバーに↑↓マークが表示されたら、ステータスバーを下方向になぞって、通知パネルを開きます。**

2 **「最新バージョン」というメッセージが表示されます。**
表示されたメッセージをタッチします。

3 **弊社 web サイトにアクセスし、最新版のプログラムをダウンロードします。**

http://appstore.elecom.co.jp/download/ikarus_free.html

本製品のアンインストール

本製品をアンインストールときは、次の手順で行います。

1 メイン画面で「アンインストール」をタッチします。

2 [はい]をタッチします。

3 パスワードを入力して、[OK]をタッチします。

4 [OK]をタッチします。
本製品のアンインストールが終了します。

こんなときは

Q 「インストールはブロックされました」という画面が表示される

A 提供元不明のアプリケーションのインストールを許可にする必要があります。[設定]をタッチして、提供元不明のアプリがインストールできるように設定してください。設定については詳しくは「端末の設定」(5 ページ)をご覧ください。

Q ダウンロードできない

A 回線が不安定な場合は、エラーが起きやすくなりますので、安定した回線状態でダウンロードしてください。

その他、よくある質問に関しては、弊社 Web サイトをご覧ください。

FAQ URL : http://app.elecom.co.jp/index.html

商品に関するお問い合わせは

【よくあるご質問とその回答】
www.elecom.co.jp/support
こちらから「製品 Q&A」をご覧ください。

【お電話・FAX によるお問い合わせ(ナビダイヤル)】

エレコム総合インフォメーションセンター
TEL : 0570-084-465
FAX : 0570-050-012

[受付時間]
9:00 ～ 19:00
年中無休

IKARUS SECURITY ソフトウェア使用許諾及びサービス契約書

本契約書を注意してお読みください。提供されたソフトウェアをインストールすることにより、以下の許諾条件に合意されたものとします。条件に合意されない場合、インストール処理をキャンセルし、配布されたソフトウェアをそれ以上使用しないでください。許諾条件に違反することは著作権侵害と見做され、民事及び刑事訴追となる場合があります。

1. 使用許諾
1.1. 使用許諾者は、IKARUS Security Software GmbH です。本使用許諾契約書は、CD、DVD、又はその他の磁器やデジタルメディアに含まれるプログラム、また被許諾者に提供されるプログラム記述、操作マニュアル及び書類に対する譲渡不能及び非独占の使用権の条件について示します。明確にするため、以下パッケージ全体を「ソフトウェア」と言及するものとします。
1.2. 本契約書の条件は、今後のソフトウェアアップデートにも適用されます。本使用許諾契約の締結により、提供されたソフトウェアの定期アップデートを含め、サービス契約にも合意したものとします。

2. 使用許諾の範囲
2.1. 本ソフトウェアは、1 カ所で 1 つのコンピューターシステム(1 つの中央 CPU)、又は 1 台のモバイル機器で、本契約条件の下においてのみ使用することができます。ネットワークを介してや、複数の PC 上でソフトウェアを使用することは、追加のマルチクライアント、又はソフトウェアを使用する PC の台数分のネットワークライセンスを購入しない限り許可されていません。これらのライセンスを所有しない場合、この点においての契約を IKARUS Security Software と締結し、必要数の追加ライセンスを購入するものとします。本ソフトウェアを他のコンピューターに添付転送することは許可されません。特に、1 クライアント又はマルチクライアントのソフトウェアライセンスをいかなる種類であれ第三者団体に提供することや、無料の場合も、直接又は間接で支払いを受ける場合も、いずれも使用を可能にすることは許可されません。サーバー上でいかなるソフトウェアも、ウイルスや同様のプログラムを検査するために、第三者団体のデータ通信をスキャンする目的で使用することは、それが被許諾者の契約上の共同経営者(例：アクセスするお客様、メールボックスのクライアント)であっても許可されません。この目的でソフトウェアを使用するには、書面での使用許諾者の同意が必要です。
2.2. 本ソフトウェアの CD、DVD、又はその他の磁器やデジタルメディア、その他コピーは、個人使用目的でも、弊社の書面による合意がなければ譲渡することはできません。法的に認められている強制介入以外で、本ソフトウェアを逆コンパイル、リバースエンジニアリング、逆アセンブル又はその他の人が認知できる形式に分解することはできません。さらに、本契約書で許可されるか法律で定められない限り、いかなる手法の使用でも、無料又は有料のいずれの場合も、合意の有無に関わらず、ソフトウェアを修正、改造、解析、販売、又は第三者団体に譲渡することはできません。

3. 保証
3.1. IKARUS Security Software は、ソフトウェアが本書で定義する最新の状態で出荷時に正常に作動することを、想定される全アプリケーションの要件を順守しているかによらず保証します。お客様は、現在の最新技術ではエラーのないソフトウェアを開発できないことを理解し合意します。これは特に、アンチウイルスプログラムからの検知を防ぐように作成された新しいウイルス、トロイの木馬、ワームや同様のプログラムに対するアンチウイルスの保護分野に適用されます。
3.2. 従って、IKARUS Security Software はソフトウェアがお客様の全要件を満たし、ソフトウェアの機能が破壊されることなく、データ、プログラム及び IT システムの全ての組み合わせでエラーなしに使用でき、また、ソフトウェアのデバッグが他のソフトウェアエラーによって発生しないことを保証しません。さらに、不適切な操作、送信中の損傷、運用システムのエラー、運用システムコンポーネント、インターフェース及びパラメーターの修正、不適切な組織のツールやデータメディアの使用によるエラー、破壊又は損傷に対して保証しません。
3.3. お客様又は第三者団体が、書面による合意なくソフトウェアの修正又は修理を行った場合、保証は終了します。また、IKARUS Security Software はそれに関連する費用を認めることはありません。修正、アップグレードや損傷、又は契約で規定した使用条件以外の方法で使用したソフトウェアに対して、修正、アップグレード又は損傷が、損害に関与していない場合を除き、保証しません。
3.4. ソフトウェアの不良に対する通知は、検知されてから 8 日以内(小売店のお客様の場合、法定通知期間内)に書面で提出する必要があります。これ以外の場合、保証は失効するものとします。双方の合意により、保証期間は小売店のお客様の場合は 2 年間、その他のお客様は 6 カ月間です。

4. 損害賠償請求 :
4.1. IKARUS Security Software に対して主張する全ての損害賠償請求は、悪質又は重大な過失で責任が法的に定められた場合を除き、除外されます。特に現在の最新技術で、誰にでも使用できるウイルス保護を提供できないウイルス又は同様のプログラムによって生ずる損害は、責任から除外されます。利益損失を含む結果的損害及び間接的損害に対する責任も除外されます。無許可の第三者団体の修正に起因する損害、また不適切な操作やインストールに対する責任も除外されます。
4.2. IKARUS Security Software は、お客様がご使用のコンピューターでファイルのバックアップを定期的に作成されることを明確にお勧めします。お客様が損失を回避、最小化又は軽減する義務を怠った場合、義務不履行によるいかなる損害にも責任を負うものではありません。重大な過失又は悪質な要因による損害が発生した場合、この損害制限は適用されません。バックアップのコピーを作成しない場合、補償を決定する際に寄与過失として考慮されます。

5. 使用許諾契約書の開始日及び期間 :
5.1. 本契約書は両当事者の合意を得た上で効力が生じます。ただし、ご使用の PC に本ソフトウェアを実際にインストールするより前の日付とします。明確な双方の合意は、郵便、E メール又は個人的に書類を受け取る、或いはお客様が受け渡すことによって書面で行われます。
5.2. 本契約書は契約上の両当事者が、特約で最初に合意した最少の条件で遂行されます（送り状を参照）。満了時は、本契約の条件によって延長されます。本契約期間中、IKARUS Security Software は継続して配信したソフトウェアの最新アップデートを、お客様に提供するものとします。具体的には、本ソフトウェアがご使用のコンピューターで、既知のウイルスや同様の脅威を検知できることを保証します。必要なプログラムアップデートは、お客様が事前に指定したアドレスに送信されます。また、オンラインアップデートのために、IKARUS Security Software のウイルスデータベースにアクセスすることもできます。お客様に提供する本製品のパスワードは、納品時に含まれています。
5.3. 手数料は使用許諾及びサービス契約の一部として定期的に実施される更新に合意します。IKARUS Security Software は価格を変更する権利を保有します。値上げが発表される場合、お客様は契約の通知期間に従って、契約を終了する権利を有します。
5.4. 本契約書はお客様が選択された使用許諾期間実施されるものとし、契約年終了前 2 カ月の通知期間に基づいて終了しない限り、満了時にその使用許諾期間で延長されます。小売店のお客様は、最初の契約年は終了時に、その後の契約年では 6 カ月ごとに通知期間に基づいて、本契約書を終了する権利を有します。契約満了後に本ソフトウェアを継続して使用することは許可されません。お客様は元の CD 及びそのコピー、付属文書を処分する義務があります。契約終了日後に本ソフトウェアを継続して使用することは、著作権侵害を意味します。
5.5. お客様が本契約書の条件、特にここでお客様に付与された権利の範囲に関して違反する場合、IKARUS Security Software は本契約書を即有効で遅延することなく終了する権利を与えられます。この場合、いかなる種類であれソフトウェアの継続使用は許可されません。

6. 最終規定 :
6.1. 国連国際物品売買条約ではなく、オーストリアの法律が本契約書に適用されます。本契約書やその満了によって起こるあらゆる紛争を扱う裁判地は、ウィーンに所在する管轄商事裁判所となります。小売店のお客様はこの対象ではなく、管轄区域の公判廷となります。本契約書に対する修正や補足は、契約の両当事者が書面に正式な署名をされた場合にのみ有効となります。権利放棄の証書の場合も、これが適用されます。

本使用許諾契約書の条件に合意されない場合、いかなる契約も IKARUS Security Software との間に締結されず、お客様は本ソフトウェアをインストールも操作を行うことはできません。本ソフトウェアをインストール及び／又は操作することにより、お客様は使用許諾の条件に同意します。本契約を終了されたい場合は、IKARUS Security Software までご連絡ください。

IKARUS mobile.security
取扱説明書
2013年4月1日 第1版
エレコム株式会社

・本書の著作権は、エレコム株式会社が保有しています。
・本書の内容の一部または全部を無断で複製 / 転載することを禁止させていただきます。
・本書の内容に関するご意見、ご質問がございましたら、エレコム総合インフォメーションセンターまでご連絡ください。
・本製品を使用したことによる他の機器の故障や不具合等につきましては、責任を負いかねますのでご了承ください。
・改良などのため、商品の仕様は予告なく変更することがあります。あらかじめご了承ください。
・イラストはイメージです。実際の商品とは異なる場合がありますので、あらかじめご了承ください。
・IKARUS mobile.security は、IKARUS Security Software Gmbh の登録商標です。
・本マニュアルの内容の一部は、Google が作成、提供している(http://www.code.google.com/policies.html) コンテンツをベースに変更したもので、クリエイティブコモンズの表示 3.0 ライセンス(http://creativecommons.org/licenses/by/3.0deed.ja)に記載の条件に従って使用しています。
・本製品のパッケージ等に記載されている会社名・製品名等は一般に各社の商標または登録商標です。

©2013 ELECOM Co., Ltd. All Rights Reserved